International Journal of Information Science and Computing
Citation: *IJISC*: **12**(02): 203-212, December 2025
DOI: 10.30954/2348-7437.2.2025.7

INFORMATION SCIENCE AND TECHNOLOGY FOUNDATION

REVIEW PAPER

A Comparative Analysis of Emerging Model Technologies and Survey Studies on Machine Unlearning

Sarmistha Podder* and Saptarshi Paul

Department of Computer Science Assam University, Silchar, India

**Corresponding author: sarmisthapodder58@gmail.com*

Received: 21 Sept., 2025 **Revised:** 31 Nov., 2025 **Accepted:** 07 Dec., 2025

ABSTRACT

Machine unlearning has emerged as a critical re- search direction in response to growing concerns about data privacy, regulatory compliance, and the ethical deployment of artificial intelligence systems. With regulations such as the General Data Protection Regulation (GDPR) enforcing the"right to be forgotten,"traditional machine learning paradigms—where models permanently retain learned information—are increasingly inadequate. This study presents a comparative analysis of emerging model technologies and existing survey studies on machine unlearning, examining how contemporary architectures address data removal, privacy guarantees, and computational efficiency. The analysis categorizes unlearning techniques into exact,approximate, federated, and verification-based approaches, and evaluates their applicability across traditional machine learning models, deep neural networks, transformer architectures, and generative models. The paper further reviews major survey contributions to identify common taxonomies, evaluation metrics, and open research challenges. Special emphasis is placed on emerging generative systems and large-scale foundation models, where latent memorization and parameter complexity complicate effective unlearning. Comparative findings highlight trade-offs between computational cost, scalability, and privacy robustness, revealing that while exact unlearning ensures strong theoretical guarantees, approximate and optimization-based methods offer practical scalability for modern deep models. Additionally, the study identifies gaps in standardized verification protocols and benchmarking practices across surveys. By synthesizing current advancements and limitations, this work provides a structured foundation for future research aimed at developing efficient, verifiable, and scalable machine unlearning mechanisms for next-generation AI systems.

Keywords: Machine unlearning, Model Unlearning, Application, Comparison Framework

The recent rapid advancements in machine learning (ML) and artificial intelligence (AI) has resulted in the widespread application of data-driven models in a variety of industries, including social media, healthcare, and finance[1].

How to cite this article: Podder, S. and Paul, S. (2025). A Comparative Analysis of Emerging Model Technologies and Survey Studies on Machine Unlearning. *IJISC.,* **12**(02): 203-212.

Source of Support: None; **Conflict of Interest:** None

However, a crucial issue has surfaced because to growing worries about compliance with regulations such as the General Data Protection Regulation (GDPR) and data privacy the requirement to eliminate particular data or user information from trained models without completely retraining them. The goal of this new field of study, called machine unlearning, is to make it possible for models to effectively and safely "forget" previously learned knowledge[2].

The purpose of unlearning machines is to provide frameworks and algorithms that can prevent or lessen the impact of specific training data. For large-scale systems, traditional retraining from scratch is frequently unfeasible because to its high computational cost. In order to accomplish effective data removal while preserving model performance, researchers have suggested a number of strategies, such as SISA (shared, isolated, sliced aggregation), knowledge distillation, gradient modification, and differential privacy-based unlearning. The accuracy, scalability, and privacy standards compliance of these approaches vary[1].

Aspects of the training data are frequently "remembered" by machine learning (ML) systems. This is problematic in many contemporary usage scenarios: users may ask for data to be deleted (the "right to be forgotten"), or data may become corrupted, out-of-date, or susceptible to policy changes. It is insufficient to simply remove data from the training set since the model may include representations of the deleted data or maintain influence. Consequently, machine unlearning (MU) has become a new paradigm for research[3].

In general, the phrase describes strategies or system architectures that cause a trained model to no longer reflect—or reflect to a satisfactory extent—the contribution of particular data points. The concept of effective unlearning for specific learners was first presented in early foundational work such Moving Towards Machine Unlearning to Make Systems Forget[4].

Machine unlearning objective, a new field of artificial intelligence research, is to effectively extract certain data or learned information from models that have been trained. Data security, ethical AI principles, and privacy rules are driving forces behind this.

Numerous survey articles have been produced to classify and assess unlearning strategies, ranging from privacy-preserving and regulation-aware frameworks to centralized and federated learning.

However, one must consider the model's applicability, cost, utility loss, and guarantee kind while choosing a technique. Instead than just identifying technologies and published articles, this survey focuses on comparing them[4].

A thorough examination of these surveys is necessary to comprehend the development of the field, pinpoint important methodologies, and identify current research gaps. This study offers an integrated understanding of how machine unlearning has advanced over time by examining their taxonomies, model technologies, and evolution criteria. In order to provide insight into the issues that need to be resolved for the practical implementation of unlearning in real-world AI systems, the findings seek to identify trends in efficiency, security, and ethical compliance.

CAUSES OF MACHINE UNLEARNING

Users may choose to remove their data from a system for various reasons, which can be grouped into four major categories: Confidentiality, security, faithfulness, and usability.

(A) Security: It has recently been demonstrated that deep learning models are susceptible to outside

threats, particularly hostile ones. An adversarial attack occurs when the attacker produces hostile data that is so identical to the original data that it is difficult for a human to distinguish between them. These hostile data are intended to compel deep learning networks to produce incorrect predictions, which frequently lead to major issues. For example, in the medical industry, a wrong forecast could lead to an improper course of treatment, an inaccurate diagnosis, or even death. Thus, recognizing and removing hostile data is essential to ensuring the model's security. The model must be able to use a machine unlearning technique to remove the hostile data once an attack has been detected[2].

(B) Confidentiality: Laws like the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) are key examples of today's privacy-focused regulations that deal with "the right to be forgotten." In order to preserve their privacy, consumers must have the option to have their data and linked information removed under this specific rule. Privacy leaks have contributed to the emergence of this legislation. For instance, cloud platforms can accidentally expose user information due to having several copies of the same data stored across different systems, backup procedures, and replication processes. In different instance, it was discovered that ML techniques for processing genomic data exposed patients' genetic markers. In order to lessen the likelihood of a data breach, it makes natural that customers would want to erase their data[2].

(C) Usability: Individuals have varying tastes when it comes to online services and/or apps, especially recommender-based systems. If an application can't completely eliminate the erroneous data (such noise, malicious data, or Out-of-Distribution (OOD) data) connected to a user, it will generate unpleasant recommendations. For instance, even after clearing his online browser history, unintentionally searching for illegal goods on his laptop, a person can find that this product recommendation keeps showing up on his phone. Not only would this undesirable usability lead to incorrect predictions, but it will also result in fewer users[2].

(D) Faithfulness: Biased machine learning models may be the source of unlearning requests. Despite recent improvements, machine learning models are still prone to bias, which means that their output may unfairly discriminate against a group of people. For instance, even though racial data is not included in the input, Studies have shown that individuals from Black communities often receive higher risk scores than their white counterparts according to COMPAS, the tool used by courts to decide parole cases. Similar circumstances have been seen in face recognition software that misread Asian face features and AI-judged beauty pageants that discriminated against contestants with darker skin tones[2].

Data is frequently the source of these biases. For instance, when processing photographs of black people, AI programs that were developed using publicly available datasets, such as Image Net, which are primarily composed of white people, are likely to make mistakes. Similar to this, the ML model in an application screening system may inadvertently pick up on unsuitable characteristics, including the gender or race of candidates. Consequently, these data, comprising the features and impacted data items, must be unlearned**.**

LITERATURE REVIEW

As researchers work to create models that can effectively forget particular inputs while maintaining overall performance, machine unlearning has garnered a lot of attention. Between 2021 and 2025, a number of studies have presented various frameworks and technologies that address this issue from many angles, including privacy, scalability, efficiency, and regulatory compliance.

SISA (sharded isolated, sliced aggregation) framework, which was one of the first and most influential approaches. This technique separated the training data across several shards, enabling the impacted portions to be selectively retrained in response to deletion requests. Compared to comprehensive retraining, SISA guarantees precise unlearning and lowers computing costs; nonetheless, its efficiency degrades when working with big or continuously updated datasets[1].

A taxonomy of exact and approximate unlearning approaches was published in later research, they focused on approximate techniques that offer faster response times at the expense of mirror accuracy trade-offs, such as gradient innovation and knowledge distillation[3].

Pruning-based unlearning, which involves removing unnecessary neurons or parameters to delete specific knowledge. This method achieves efficiency but occasionally causes performance instability.

Federated machine unlearning was investigated by AI to solve data removal among decentralized clients. This paradigm advanced privacy-preserving systems by utilizing safe aggregation and local retraining to preserve privacy in collaborative settings[2].

In order to create privacy-aware unlearning frameworks that adhere to the GDRP's "right to be forgotten" while maintaining interpret ability and model utility, more recently combined differential privacy with model compression techniques[5].

In contrast, newer technologies prioritize privacy guarantees, scalability, and regulatory compliance, while earlier models concentrated primarily on retraining efficiency and data isolation. Despite these developments, difficulties still exist in ensuring provable unlearning, creating unified benchmarks, and minimizing performance loss. For machine unlearning to be practical for real-world AI applications, future research must strike a compromise between computational efficiency and robust privacy assurance.

THE UNLEARNING ALGORITHMS

(A) Model-agnostic methods

Machine unlearning procedures or frameworks that function with several models are examples of model-agnostic machine unlearning techniques. Theoretical assurances, however, are sometimes limited to particular model classes (e.g., linear models).However, because their fundamental concepts apply to intricate models (like deep neural networks) and have real-world applications, they are still regarded as model-agnostic[2].

1. Distinctive privacy: Differential privacy has historically reduced the influence of data samples on machine learning models. Differential privacy can also be utilized in machine unlearning to lower the degree of variation in the relevant model parameters by changing parameters to forget the data samples[2].

2. Learning through statistical queries: A type of machine learning called statistical query learning uses a model can be trained using statistical summaries derived from the data instead of relying on the raw data itself. When certain data points need to be removed, the statistical information can simply be recomputed using only the remaining samples. This approach enables the model to "forget" specific data effectively, without requiring access to the original removed records[3].

3. MCMC unlearning (sampling parameters): It is another method used to help a machine learning model forget certain training data. The idea is to use Markov Chain Monte Carlo (MCMC) to sample

the model's parameter distribution. This works well when the amount of data that needs to be forgotten is very small compared to the full training set—because if too much data must be removed, retraining the whole model is usually better. With this approach, the model's parameters after unlearning stay very close to what they were before, so the model behaves almost the same, just without the unwanted data[2].

(B) Model-intrinsic techniques: Most model-intrinsic methods are unlearning techniques created for particular kinds of models. Even though these methods are tailored to specific model types, they can still be widely used because many machine learning models share similar structures and characteristics[3].

1. Softmax classifiers (probability-based classifiers): The softmax classifier is a widely used machine learning method for handling problems with multiple classes. It works by turning the model's raw outputs into a probability distribution, showing how likely each class is. In softmax-based unlearning, the goal is to adjust the model's parameters so that the removed data no longer affects its predictions. This usually means recalculating and updating the model's weights to ensure they no longer represent the patterns or features of the data that has been deleted[2].

2. Techniques to remove data influence from linear models: In machine learning, unlearning in linear models refers to removing the effect of certain data points from a trained linear model without having to train it again from scratch. Models like linear regression and logistic regression use every data point during training, so their parameters reflect all the input samples. Therefore, to make the model forget specific data, the model's parameters must be carefully updated so that those removed points no longer influence the model's behavior[2].

3. Tree-based modeling with machine unlearning: A classification method called tree-based modeling divides the feature space recursively. These models is based on certain measures, like information gain, which help decide which features and threshold values should be used for classification. Extreme Random Trees, a type of tree-based model, are built from multiple decision trees. They work well because both the feature choices and the split thresholds are chosen randomly. To keep the process efficient, the model picks the best splits by minimizing Gini impurity, which avoids the heavier calculations required by logarithmic measures[3].

4. Bayesian machine unlearning modeling: A probabilistic model for estimating posterior probabilities is called a Bayesian model. This technique often referred to as Bayesian inference is especially helpful when the loss function is unclear or not defined well. Many machine learning methods belong to the broader family of Bayesian models, including Bayesian neural networks (which apply Bayesian principles to neural nets), probabilistic graphical models (which show variable relationships through graphs), generative models, topic modeling methods, and probabilistic matrix factorization techniques. Unlearning in Bayesian models is more complex because their training process focuses on refining the posterior distribution of the model's parameters, which requires careful adjustments when certain data must be forgotten[2].

5. DNN-based machine unlearning: Models that automatically extract features from data are called deep neural networks. Because of this, It is often challenging to pinpoint how much each individual data sample contributes to updating a model. However, deep neural networks contain many layers, which makes this task more manageable. For layers that use convex activation functions, existing unlearning techniques—such as certified removal methods—can be applied directly. For the non-convex layers, a caching strategy is used: the model is first trained on data that will never need to be forgotten, and later

fine-tuned on user-specific data using specialized convex optimization methods. This helps ensure that user data can be removed effectively when needed[3].

(C) Data-driven techniques: Lean analysis, data closure are the main principles of the data-driven approach. To establish a cycle of positive feedback, promote algorithm optimization, and implement a data-centric method for machine unlearning, data is collected and utilized as production data through business processes and data mining techniques. This data helps refine patterns and generate insights, which are then applied to improve the algorithm[2].

1. Partitioning data (effective retraining): Techniques for Data Partitioning (Effective Retraining) to expedite the retraining process, categories employ data segmentation techniques. As an alternative, they set specific accuracy limitations and partially retrain the model. The widely used SISA framework splits the data into sub slices and partitions. The final output is the sum of the results of several models on various divisions, each of which has its own model. In order to retrain a new model from an interim state, a model checkpoint is saved for each partition's sub-slice throughout training[3].

2. Improvement of data: Increasing the amount of data to aid in model training is known as data augmentation, and same technique can also be applied to machine unlearning. It functions by causing the model to disregard the given dataset as if it contains no useful information. However, It is restricted to protecting specific data points before model training[2].

3. Impact of data: The Data Influence type of machine learning algorithms uses an influence function to measure how changes in the training data affect the model's parameters. However, this function relies on the model's current state, which can make it less reliable over time. To solve this issue, researchers have suggested keeping a record of the training history including intermediate values like gradients or model parameters created during each step of training. During the unlearning process, these stored updates can then be reversed or subtracted to help the model forget specific data[3].

4. Evaluation of algorithms: Accuracy, completeness, unlearning time, and other measures are frequently used to evaluate anomaly and detection performance in machine unlearning[2].

APPLICATION OF MACHINE UNLEARNING

1. Compliance and Data Privacy: GDPR and CCPA Compliance by eliminating user data and its impact from machine learning models, MU assists businesses in adhering to "right to be forgotten" regulations.

2. User Consent Withdrawal: Without retraining the entire model, MU may effectively remove users' data impact when they withdraw their consent[2].

3. Confidentiality and Security: Data Poisoning Removal: MU can improve model reliability by eliminating the impact of faulty or malicious data. Assists in removing private or sensitive training data that was inadvertently included (such as private financial or medical information[2].

4. Updating and Maintaining Models: Effective Model Refresh: MU can update models by deleting out-of-date or unnecessary data, as opposed to completely retraining them. Adaptive learning systems are helpful in systems (like spam filters and recommended systems) where data is constantly changing[2].

5. Distributed and Federated Education: MU allows the removal of contributions from particular clients or users without global retraining in federated learning, when models are trained across various devices or organizations[2].

6. Correction of Bias and Fairness: makes ML systems more moral and impartial by assisting in the removal of biased samples or groups that cause discrimination in models[2].

7. Sensitive Domains and Healthcare: MU makes sure that models used for diagnosis or prediction safely and morally reflect any changes that must be made to patient data[2].

PROBLEM STATEMENT

Data deletion is difficult after a model has been trained. Because it is computationally costly to retrain from scratch, effective unlearning methods are required. This study compares and assesses the underlying model technology of a rising number of survey studies that review various approaches.

OBJECTIVES

In order to examine current research articles on machine learning (2020–2025).

- ❒ To contrast how they classify unlearning techniques.
- ❒ To determine which model technologies—such as knowledge distillation, SISA, incremental learning, and differential privacy—were employed in their assessment.
- ❒ To draw attention to future trends and research gaps.

METHODOLOGY

1. Data Collection: First a standard cyber security dataset will be selected such as NSL KDD or CIC IDS. This dataset will contain normal and attack traffic like DDoS and Botnet.

2. Data Pre processing: The collected data will be cleaned and filtered. Missing values will be handled. Irrelevant features will be removed. Data will be normalized so that it can be used by deep learning models.

3. Model Development: A deep learning model will be designed for IDS such as CNN or LSTM. The model will be trained using the processed dataset to learn attack patterns.

4. Attack Detection: The trained model will be tested to detect and predict cyber attacks. Performance will be measured using accuracy precision recall and F1 score.

5. Poisoned Data Injection: Some poisoned or wrong data samples will be added into the training set to simulate data poisoning attacks. The impact on model accuracy will be observed.

6. Machine Unlearning Implementation: Machine Unlearning techniques such as SISA or Gradient Ascent will be applied to remove the influence of selected poisoned or outdated data from the model.

7. Performance Evaluations: After unlearning the model performance will be tested again. Results will be compared before and after unlearning. Unlearning time and accuracy will be analyzed.

8. Result Analyses: The final results will be analyzed to show how Machine Unlearning improves IDS performance and reduces the effect of poisoned and outdated data.

COMPARATIVE FRAME WORK

Year	Authors	Technology/ Method	Type of Unlearning	Advantages	Limitations
2021	Bourtoul *et al.*	SISA framework (hared, isolated, sliced Aggregation	Exact	Modular design, efficient retraning	Poor scalability for large models
2022	Nguyen *et al.*	Gradient & knowledge Distillation Method	Approximate	Fast unlearning, simple implementation	Accuracy degradation
2023	Warneck *et al.*	Pruning – Based unlearning	Approximate	Reduce model size computationally light	May affect model stability
2024	Zhang & *et al.*	Federated Machine unlearning (F L unlearning)	Federated/ Distributed	Privacy-presenting, suitable for multi-client systems	High Communication cost
2025	Kim *et al.*	Privacy – Aware unlearning (DP + Model compression	Privacy-preserving	GDPR compliance, maintains privacy and efficiency	Requires fine-tuning to balance accuracy

DISCUSSIONS

- Trend 1: transition from Federated Unlearning (2024–2025) to Centralized Unlearning (2021).
- Trend 2: Using approximation unlearning to strike a compromise between speed and accuracy.
- Trend 3: Using knowledge distillation and differential privacy to create safe, lightweight unlearning.
- Trend 4: Evaluation measures are developing beyond accuracy to incorporate privacy assurances and energy costs.

FUTURE DIRECTIONS

- A consistent framework for benchmarking to ensure fair comparison.
- AI models with regulatory awareness that provide verifiable unlearning
- Explainable unlearning for increased openness.
- Unlearning across domains (e.g., vision to language models).

CONCLUSION

Machine unlearning has become an essential research area as artificial intelligence systems continue to expand into sensitive and large-scale applications. This comparative analysis shows that while traditional

machine learning models allow relatively structured and manageable unlearning processes, emerging model technologies—such as deep neural networks, transformer-based architectures, and generative models—introduce greater complexity due to their high dimensional parameter spaces and latent knowledge representations. Existing survey studies provide strong taxonomies and categorizations of unlearning approaches, typically dividing them into exact, approximate, federated, and verification-based techniques. However, many surveys focus more heavily on classical and discriminative models, with limited standardized evaluation frameworks for large generative systems.

The findings indicate that exact unlearning methods offer stronger theoretical guarantees but are often computationally expensive, making them less practical for modern large-scale systems. In contrast, approximate and optimization-based techniques are more scalable but may leave residual information, raising verification concerns. Additionally, the lack of universally accepted benchmarks and auditing metrics remains a significant challenge. Overall, while survey studies have laid a solid foundation for understanding machine unlearning, further research is needed to develop scalable, efficient, and provably reliable unlearning mechanisms suited for emerging AI technologies.

REFERENCES

1. Bourtoule, L., Chandrasekaran, V., Choquette-Choo, C.A., Jia, H., Travers, A., Zhang, B. and Papernot, N. 2021. Machine unlearning. In 2021 IEEE symposium on security and privacy (SP) (pp. 141-159). IEEE.

2. Li, C., Jiang, H., Chen, J., Zhao, Y., Fu, S., Jing, F. and Guo, Y. 2024. An overview of machine unlearning. *High-Confidence Computing,* **5**(2): 100254.

3. Nguyen, T.T., Huynh, T.T., Ren, Z., Nguyen, P.L., Liew, A.W.C.,Yin, H. and Nguyen, Q.V.H. 2022. A survey of machine unlearning. *ACM Transactions on Intelligent Systems and Technology,* **16**(5): 1-46.

4. Warnecke, A., Pirch, L., Wressnegger, C. and Rieck, K. 2023. Machine unlearning of features and labels. arXiv preprint arXiv: 2108.11577.

5. Kim, M., Yang, N. and Jung, K. 2025. Rethinking Post-Unlearning Behav-ior of Large Vision-Language Models. arXiv preprint arXiv:2506.02541.

6. Huang, A., Cai, Z. and Xiong, Z 2025. A Survey of Machine Unlearning in Generative AI Models Methods Applications Security and Challenges. *IEEE Internet of Things Journal,* **12**(16): 32563-32580.

7. Liu, Z., Ye, H., Chen, C. and Zheng, K.Y. 2024. Lam Threats Attacks and Defenses in Machine Unlearning A Survey. *IEEE Open Journal of the Computer Society*.

8. Xue, L., Hu, S., Lu, W., Shen, Y., Li, D., Guo, P., Zhou, Z., Li, M., Zhang, Y. and Zhang, L.Y. 2025. Towards Reliable Forgetting A Survey on Machine Unlearning Verification Challenges and Future Directions arXiv 2506 15115 2025.

9. Shaik, T., Tao, X., Xie, H., Li, L., Zhu, X and Li, Q. 2023. Exploring the Landscape of Machine Unlearning A Comprehensive Survey and Taxonomy. arXiv 2305 06360 2023.

10. Song, B., Zhao, D., Xiang, J., Xu, Q. and Yu, Z. 2025. Injection Attack and Erasure Revocable Backdoor Attacks via Machine Unlearning. arXiv 2510 13322 2025.

11. Brodzinski, C.E.J. 2024. Survey of Security and Data Attacks on Machine Unlearning in Financial and E Commerce *arXiv* 2410 00055 2024.

12. Cao, Y. and Yang, J. 2015. Towards Making Systems Forget with Machine Unlearning. *IEEE Symposium on Security and Privacy.*

13. Liu, Y. *et al*. 2024. "Machine Unlearning for Federated Learning-Based Intrusion Detection Systems," *IEEE Transactions on Information Forensics and Security,* **19**: 3157-3171.

14. Wang, H. *et al.* 2024. "Adversarial Data Removal in Network Intrusion Detection Systems via Certified Machine Unlearning," *IEEE Transactions on Dependable and Secure Computing,* **21**(3): 1454-1469.

15. Yang, K. and Chen, J. 2024. "Poisoned Sample Elimination for Robust Malware Classification Using Gradient-Based Machine Unlearning," *IEEE Transactions on Neural Networks and Learning Systems,* early access, 2024.

16. Sun, L. *et al.* 2024. "Adaptive Cyber Attack Prediction via Selective Forgetting in Recurrent Neural Networks," *IEEE Transactions on Knowledge and Data Engineering,* **36**(5): 2112-2125.

17. Zhang, R. *et al.* 2024. "Efficient Unlearning for Deep Learning-Based IoT Anomaly Detection," *IEEE Internet of Things Journal,* **11**(8): 13874-13887.

18. Gupta, S. *et al.* 2024. "SISA-Inspired Unlearning for Real-Time Intrusion Detection Under Evolving Attack Patterns," *IEEE Transactions on Network and Service Management,* **21**(1): 492-506.

19. Xu, M. *et al.* 2024. "Machine Unlearning in Graph Neural Networks for Dynamic Network Security Analysis," *IEEE Transactions on Network Science and Engineering,* **11**(2): 1865-1878.

20. Zhao, P. *et al.* 2024. "Unlearning Backdoor Attacks from Deep Learning Based Phishing Detectors," *IEEE Transactions on Computational Social Systems,* early access, 2024.

21. Li, T. *et al.* 2024. "Verifiable Unlearning for Privacy-Preserving Collaborative Threat Intelligence Sharing," *IEEE Transactions on Big Data,* **10**(1): 224-238.

22. Rajput, A. and Singh, B.K. 2024. "Incremental Learning with Selective Forgetting for Adaptive DDoS Detection," *IEEE Communications Letters,* **28**(1): 161-165.

23. Chen, C. *et al.* 2024. "Federated Unlearning for Edge-Based Attack Prediction in Industrial Cyber-Physical Systems," *IEEE Transactions on Industrial Informatics,* **20**(4): 6103-6114.

24. Menon, V.G. *et al.* 2024. "Machine Unlearning to Mitigate Data Poisoning in 5G Network Slice Security Analytics," *IEEE Transactions on Vehicular Technology,* **73**(1): 1125-1139.

25. Altaf, F. *et al.* 2024. "A Certified Data Removal Framework for Cloud-Based Security Information and Event Management (SIEM) Systems," *IEEE Transactions on Cloud Computing,* **12**(1): 543-557.

26. Goel, G. *et al.* 2023. "Forgetting to Enhance Robustness: Machine Unlearning Against Adversarial Examples in Cyber Attack Classifiers," *IEEE Access,* **11**: 134209-134223.

27. Park, J. and Lee, S. 2023. "Lifelong Learning with Strategic Forgetting for Malware Traffic Classification," *IEEE Wireless Communications Letters,* **12**(10): 1775-1779.